Installation du module TPM après RMA du châssis SNS3700

Table des matières

Introduction

Considérations

Problème

Solution

- Installer le matériel du module de plateforme sécurisée et l'activer dans le BIOS
- Activer le module dans CIMC
- Mise hors tension puis sous tension du serveur et réinitialisation de CIMC
- Vérifier que CIMC détecte le module comme étant équipé et activé
- Réinstaller l'application ISE

Vérification

Introduction

Ce document décrit le processus d'installation du module TPM sur les serveurs SNS3700 qui ont obtenu un remplacement du châssis.

Considérations

Le module de plateforme sécurisée (TPM) est un composant matériel qui améliore la sécurité du serveur en stockant des clés de cryptage.

Néanmoins, le serveur peut exécuter Identity Services Engine (ISE) sans sa présence.

⚠ Mise en garde : Si l'application ISE est installée et qu'elle s'exécute sur un serveur sans TPM, vous devez exécuter le processus décrit ici pour installer le module et le rendre utilisable par le système.

- Ce serveur prend en charge TPMversion 2.0 (UCSX-TPM-002C) tel que défini par le groupe TCG (Trusted Computing Group). Le TPM est également basé sur SPI.
- Impossible de remplacer le TPM. Autrement dit, si le module est déjà installé, il ne peut pas être retiré et remplacé car il est installé avec une vis inviolable.
- Si le module de plateforme sécurisée (TPM) est absent de la carte mère, un module peut être installé.

- Si un serveur avec un TPM est retourné, le serveur de remplacement doit être commandé avec un nouveau TPM.
- Si TPM2.0 ne répond plus, redémarrez le serveur.

Problème

La gamme SNS 3700 ou supérieure, livrée par Cisco Manufacturing, inclut un module TPM.

Toutefois, les châssis de remplacement de la gamme SNS 3700, expédiés depuis les Dépôts de services Cisco, ne sont pas fournis avec ce type de périphérique.

Le processus suivant doit être exécuté pour installer le module de plateforme sécurisée et permettre au matériel et aux logiciels de tirer parti des avantages du module.

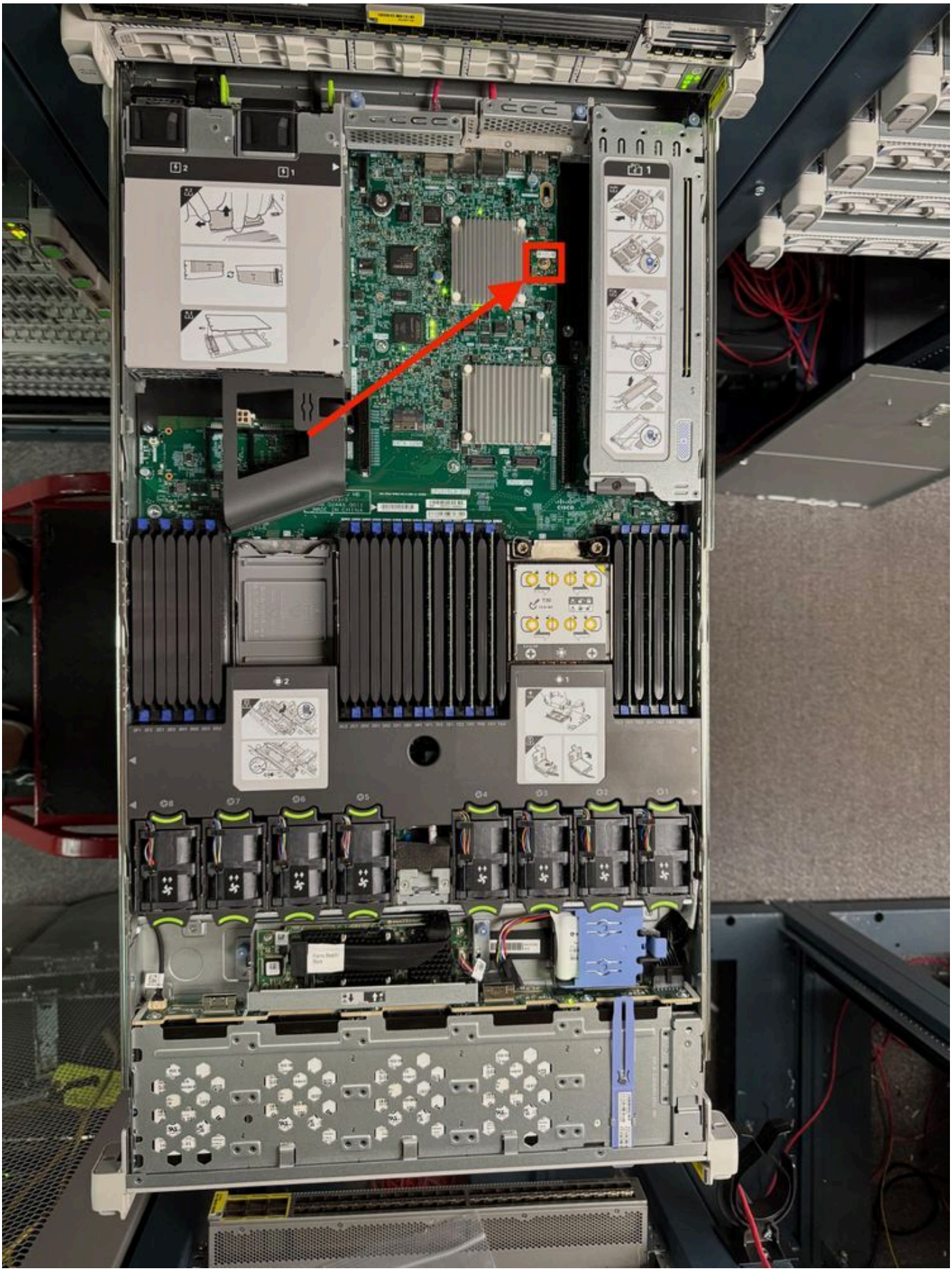


Image 1. Emplacement du module TPM dans l’appareil SNS 3700

Solution

Exécutez les étapes suivantes dans l'ordre indiqué pour installer le module, l'initialiser et tirer parti des fonctions de sécurité qu'il fournit.

Installer le matériel du module de plateforme sécurisée et l'activer dans le BIOS

Utilisez cet article pour effectuer les étapes 1 : Guide d'installation et de maintenance du serveur Cisco UCS C220 M6 - Maintenance du serveur

Le processus est terminé une fois que vous avez terminé les étapes du chapitre Activation du module de plateforme sécurisée du BIOS.

Activer le module dans CIMC

Connectez-vous à CIMC.

Cliquez sur l'icône de menu > Compute > Configure BIOS > Security > Change the Trusted Platform Module State to Enabled.

Cliquez sur Save.

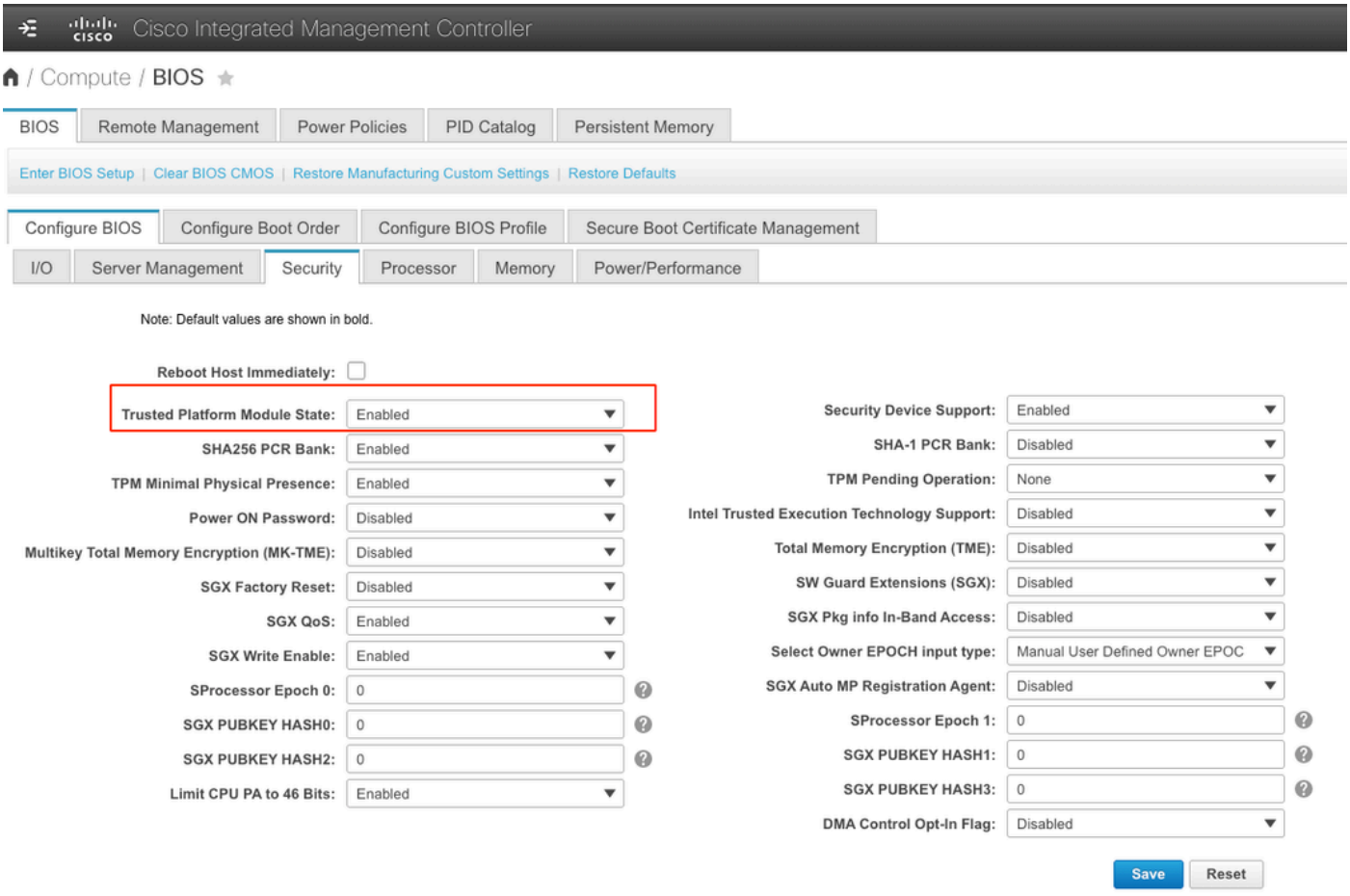


Image 2. Activation du module de plateforme sécurisée dans CIMC

Mise hors tension puis sous tension du serveur et réinitialisation de CIMC

En haut de l'interface CIMC, cliquez sur Host Power.

Sélectionnez Power Cycle.

Attendez 5 minutes.

En haut de l'interface CIMC, cliquez sur CIMC Reboot.

Attendez que le CIMC revienne.

Vérifier que CIMC détecte le module comme étant équipé et activé

Une fois que le CIMC est de retour, cliquez sur l'icône de menu et accédez à : Châssis > Inventaire > TPM.

Le module de plateforme sécurisée doit être détecté et les informations suivantes doivent être affichées.

Présence : Équipé

État activé : Activée

État actif : Activé



Image 3. PTSM détecté, activé et activé du point de vue de CIMC

Réinstaller l'application ISE

Pour terminer l'étape 5, accédez au lien suivant et accédez au guide d'installation de la version ISE que vous devez installer sur le serveur :

Guides d'installation et de mise à niveau - Installation de Cisco ISE

Une fois dans le guide d'installation, accédez à la section Installer Cisco ISE.

Vérification

Une fois cette étape terminée, vous devez installer et exécuter ISE.

Accédez à l’interface de ligne de commande du noeud et utilisez la commande suivante pour générer un fichier show tech.

ISE/user#show tech-support file <nom du fichier>

Vous pouvez ensuite copier le fichier sur une mise en pension à l'aide de la commande copy ou vous pouvez télécharger le fichier en accédant à l'interface graphique utilisateur et en accédant à :

Administration > Système > Maintenance > Gestion des disques locaux

Une fois que vous avez le fichier, ouvrez-le avec un éditeur de texte et vérifiez que la sortie suivante affiche le module de plateforme sécurisée comme présent.

****
Affichage du profil ISE...
****
Profil : sns3755
TPM : Module présent

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.